

8300 Greensboro Dr.  
Suite 1200  
McLean, VA 22102  
WWW.FCCLAW.COM

Pamela L. Gist  
(703) 584-8665  
pgist@fcclaw.com

**LNGS** | LUKAS,  
NACE,  
GUTIERREZ  
& SACHS, LLP

February 25, 2014

Marlene H. Dortch, Office of the Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Suite TW-A325  
Washington, D.C. 20554

Re: EB Docket No. 06-36  
Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2013

East Kentucky Network, LLC d/b/a Appalachian Wireless

Dear Ms. Dortch:

On behalf of East Kentucky Network, LLC d/b/a Appalachian Wireless, and pursuant to Section 64.2009(e) of FCC rules, submitted herewith is the carrier's CPNI certification with accompanying statement covering calendar year 2013.

Should any questions arise regarding this submission, kindly contact the undersigned.

Very truly yours,



Pamela L. Gist

Enclosure

cc: Best Copy and Printing, Inc.

**Annual 47 C.F.R. 64.2009(e) CPNI Certification  
EB Docket No. 06-36**

Annual 64.2009 (e) CPNI Certification covering 2013

Date Filed: February 25, 2014

Company Name: East Kentucky Network, LLC  
d/b/a Appalachian Wireless  
101 Technology Trail  
Ivel, KY 41642

Form 499 Filer ID: 802104

Name of signing officer: W.A. Gillum

Title of signatory: Chief Executive Officer

CERTIFICATION

I, W. A. Gillum, hereby certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Customer Proprietary Network Information rules set forth in 47 C.F.R. 64.2001 *et seq.* of the rules of the Federal Communications Commission.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

A handwritten signature in dark ink, appearing to read "W A Gillum", is written over a horizontal line.

Name: W.A. Gillum

Title: CEO/General Manager

Date: February 25, 2014

Attachment:    Accompanying Statement explaining CPNI procedures  
                     Explanation of actions taken against date brokers (if applicable)  
                     Summary of customer complaints (if applicable)

Company Name ("Carrier"): East Kentucky Network, LLC d/b/a Appalachian Wireless

## STATEMENT

East Kentucky Network, LLC d/b/a Appalachian Wireless ("Carrier") has established operating procedures that ensure compliance with the Federal Communication Commission ("Commission") regulations regarding the protection of Customer Proprietary Network Information ("CPNI").

- Carrier has designated a CPNI compliance officer to oversee CPNI training and implementation.
- Carrier has a system implemented whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.
- Carrier continually educates and trains its employees regarding the appropriate use of CPNI. Carrier has established disciplinary procedures should an employee violate the CPNI procedures established by Carrier.
- Carrier does not use its customer's CPNI in its or its affiliates' sales and marketing campaigns. Carrier does not conduct outbound marketing to its customers. Carrier does not provide an opt-in election to its customers; controls are established to automatically designate all customers as selecting an opt-out election.
- Carrier has procedures implemented to properly authenticate customers prior to disclosing CPNI over the telephone, at Carrier's retail locations or otherwise, and in connection with these procedures. Carrier has established a password system and back-up authentication methods for all customers and accounts, which complies with the requirements of applicable Commission rules.
- Carrier has procedures established to ensure that customers will be immediately notified of account changes including changes to passwords or address of record, and a back up means of authentication for lost or forgotten passwords.
- Carrier has procedures established to notify law enforcement and customer(s) of unauthorized disclosure of CPNI in accordance with FCC timelines.
- Carrier took no actions against data brokers in 2013, including proceedings instituted or petitions filed by Carrier at a state commission, in the court system, or at the Commission.
- Carrier has found that pretexters are continuing their attempts to access CPNI through phone calls and customer impersonation. Carrier's use of a passcode/pin-code to properly authenticate customers, plus additional verification procedures, protects CPNI.

- The following is a summary of all customer complaints received in 2013 regarding the unauthorized release of CPNI:

\*Number of customer complaints Carrier received in 2013 related to unauthorized access to CPNI or unauthorized disclosure of CPNI: 2

\*Category of complaint:

1 Number of instances of improper access by employees.

A customer complaint was received and following an internal investigation, it was found that someone with the account password entered a retail location without a photo ID and demanded that two lines of suspended service be turned back on. The Retail Sales Associate did not release any CPNI information but did restart the two lines of service. Though no CPNI information was released, the RSA violated an internal procedure. East Kentucky Network handled the violation in accordance with written CPNI policies and procedures by suspending the RSA for 3 days.

\_\_\_ Number of instances of improper disclosure to individuals not authorized to receive the information.

\_\_\_ Number of instances of improper access to online information by individuals not authorized to view the information.

1 Number of other instances of improper access or disclosure.

A customer complaint was received accusing an employee of releasing call detail information to someone not authorized on an account. The first time Carrier Management spoke with the account holder, he was unsure the name of the employee but knew that that his ex-wife and the employee's wife were friends. The second time Carrier Management spoke with the account holder, he gave a specific name but then was unsure if the employee had released this information. The accused employee is not in a position within the company that would have any access to call detail.